**CYNDEE L. PETERSON**
**Assistant U.S. Attorney**
**U.S. Attorney's Office**
**P.O. Box 8329 / 105 E. Pine, 2nd Floor**
**Missoula, MT 59807 / 59802**
**Phone: (406) 542-8851**
**Fax: (406) 542-1476**
**E-mail: Cyndee.Peterson@usdoj.gov**

**MAUREEN C. CAIN**
**U.S. Department of Justice**
**Child Exploitation & Obscenity Section**
**1400 New York Ave.**
**Bond Building, 6th Floor**
**Washington, D.C. 20530**
**Phone: (202) 616-1685**
**Fax: (202) 514-1793**
**Email: Maureen.Cain@usdoj.gov**

**ATTORNEYS FOR PLAINTIFF**
**UNITED STATES OF AMERICA**

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MONTANA**
**MISSOULA DIVISION**

| | |
|---|---|
| **UNITED STATES OF AMERICA,**<br><br>**Plaintiff,**<br><br>**vs.**<br><br>**JOHN MERCHBERGER III, DANIEL BROWN, MARC EDORIA, TONY GUSTAFSON, RYAN HATFIELD, RICHARD PITTS, DAVID WOODS, and SHAWNSTON BEAUDOIN,**<br><br>**Defendants.** | **CR 14- 27-M-DLC**<br><br>**GOVERNMENT'S RESPONSE TO MOTION TO SUPPRESS EMAIL ACCOUNT AND RESIDENTIAL SEARCH WARRANT EVIDENCE (DEFENDANTS EDORIA, MERCHBERGER, BROWN AND GUSTAFSON)** |

The United States, by and through Cyndee L. Peterson, Assistant U.S. Attorney for the District of Montana, and Maureen C. Cain, Trial Attorney for the U.S. Department of Justice, hereby opposes the motion to suppress the email account evidence filed by defendants Marc Edoria, John Merchberger, Daniel Brown, and Tony Gustafson. Defendants contend that the search warrants on their email accounts were overbroad, thus, all email account evidence should be suppressed, along with the subsequent residential search warrants and the items and statements obtained therein.

Defendants have failed to show that the email search warrants were overbroad. Alternatively, even if the email search warrants were overbroad, defendants have failed to show what parts of the warrant should be stricken and which parts of the email accounts should be suppressed. Contrary to defendants' suggestion, an overbroad email search warrant does not doom the entire warrant. Even if defendants were to point out what parts of the email search warrant should be suppressed, all of the evidence is admissible under *Leon*'s good faith exception to the exclusionary rule. Under *Leon*, agents acted in good faith reliance on the email search warrants presented to and signed by United States Magistrate Judge Jeremiah Lynch.

As to the residential search warrants, defendants fail to show how probable cause was lacking in the warrants if the email evidence were to be severed from the residential search warrant affidavits. Alternatively, the *Leon* good faith exception applies yet again because the agents presented the residential search warrant papers to a federal magistrate judge within their respective districts and obtained judicial approval for the warrants. Reliance on such warrants was reasonable. Accordingly, defendants' motion to suppress evidence should be rejected.

## I. FACTUAL AND PROCEDURAL BACKGROUND

This case arises out of the Dark Moon (aka DMoon) bulletin board, a web-based bulletin board which specialized in advertising, distributing, receiving, and accessing with intent to view child pornography. DMoon was created on or about September, 2011 and continued to operate through March, 2014. When becoming a member of DMoon, members provided their email addresses for board registration. By providing an email address for board registration, members were then able to receive email notifications connected to DMoon activity, including private messages.

To help determine the location of various DMoon members, agents sent out administrative subpoenas to the email providers for IP address information. The administrative subpoena returns, in addition to some open source public records checks, allowed agents to determine the location of the defendants' residences (which is where the criminal activity from the board was occurring).

Despite knowing the location of the defendants through the administrative subpoenas and public record checks, agents sought to obtain additional intelligence on the targets through search warrants on various board users' email accounts. *See* Ex. A (Merchberger email account search warrant papers for ozias21@gmail.com); Ex. B (Brown email search warrant papers for olvidadaalma@gmail.com); Ex. C (Gustafson email search warrant papers for fourteenthousandfeet@hotmail.com); and Ex. D (Edoria email search warrant papers for soarinblades@yahoo.com). The affidavits in support of the email search warrants discuss the relevant criminal charges involved in the investigation, including conspiracy to advertise, receive, distribute, and access with intent to view child pornography.

The affidavits further discuss the common characteristics of individuals involved in advertising, distributing, receiving and/or

accessing child pornography. For example, the affidavits state that such individuals often use email accounts to store, distribute and receive child pornography while also communicating with other child pornographers. *See, e.g.*, Ex. A, pgs. 9-10 para. c-d; pg. 13 (last sentence).[1] As described in the affidavits, the individuals may maintain the images of child pornography in their email accounts, along with the contact list and communications with others interested in child pornography for years, and such items are rarely destroyed. Ex. A at pg 9-10 para. c-d; pg. 13 (last sentence).

The affidavits further discuss the types of data commonly found in email accounts, including identity evidence, to assist agents in determining who is using the email account and ultimately engaging in the relevant criminal activity. Such identity evidence can be found in communications with friends and family, attached pictures, and billing information. Ex. A, pgs. 14-15. The affidavits further provide information on how web-based bulletin boards typically function, including the board notifications that can be sent to one's email account. Ex. A, pg. 14-15, para. i. The affidavits also discuss the DMoon bulletin

[1] To avoid redundancy, the Government will cite to Merchbeger's email search warrant papers. The same information cited herein was also provided in the search warrant papers for Brown, Gustafson, and Edoria.

board investigation, including the various members, and numerous specific instances of members advertising, distributing, receiving, and accessing with intent to view child pornography. Ex. A, pg. 20-56.

The attachments to the email search warrants are standard attachments routinely used. Attachment A describes the specific email account to be searched, along with information about where the email service provider is located. Attachment B has two parts. The first part of Attachment B requests that the email service provider make various forms of information associated with the account available for agents. The second part of Attachment B describes the information to be seized by agents, including "correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2251(d) & (e); 18 U.S.C. § 2252A(a)(2); 18 U.S.C. § 2252A(a)(5)(B); and 18 U.S.C. § 2252A(b)(1) & (2)." Attachment B then provides the elements for each offense. Attachment B also seeks evidence relating to identity and the times when the account was used.

Agents next prepared and executed residential search warrants on the various targets. *See* Ex. E (Merchberger Residential Search Warrant papers); Ex F (Brown Residential Search Warrant papers

SEALED); Ex. G (Gustafson residential search warrant papers SEALED); and Ex. H (Edoria residential search warrant papers SEALED).[2] When reviewing the affidavits in support of the residential search warrants, it is clear that agents were able to determine the location of where the criminal activity was occurring with each board member based on the results of administrative subpoenas for the various email accounts and public record checks alone. *See* Ex. E (Merchberger), pg. 17 para. 31; Ex. F (Brown), pg. 40-41; Ex. G (Gustafson), pg. 31 para. (g) & (h); Ex. H (Edoria), pg. 22-23 para. 44-53). While some identity information from the email search warrants is in the residential search warrant papers, the information relates to who within the residence may be engaged in criminal activity.

## II. LEGAL ARGUMENT

### A. The Email Search Warrants Were Not Overbroad.

Defendants' attacks on the email search warrants as being overbroad should be rejected. When analyzing search warrants, the affidavit in support of the search warrant incorporated therein must be

[2] The search warrants and accompanying documents for the residences of Brown, Gustafson and Edoria were sealed by the courts in their respectively districts. All of the documents have been provided to defendants in discovery but are still under seal by court order in those districts. As such, the government files those three search warrants *under seal* in this matter.

considered with the search warrant papers and attachments. In considering whether a search warrant complies with the Fourth Amendment, the warrant cannot be "overbroad." "Under the Fourth Amendment, this means that there must be probable cause to seize the particular thing[s] named in the warrant." *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 -708 (9th Cir. 2009). "[P]robable cause means a fair probability that contraband or evidence of a crime will be found in a particular place, based on the totality of circumstances." *United States v. Diaz,* 491 F.3d 1074, 1078 (9th Cir. 2007) (internal quotation marks omitted); *see United States v. Gourde,* 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc) ("[P]robable cause means 'fair probability,' not certainty or even a preponderance of the evidence.").

The description of the items to be seized in a search warrant must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized. *United States v. McClintock*, 748 F.2d 1278, 1282 (9th Cir.), cert. denied, 474 U.S. 822 (1985). The warrant's description of items need only be "reasonably specific rather than elaborately detailed." *United States v. Holzman*, 871 F.2d 1496, 1508 (9th Cir. 1989) (*quoting United States v. Storage*

*Spaces Designated Nos.* 8 & 49, 777 F.2d 1363, 1368 (9th Cir. 1985), cert. denied, 479 U.S. 1086 (1987)).

Even if a search warrant is deemed overbroad, the warrant is not doomed as a whole. Not all evidence is suppressed. Instead, the court must sever the deficient portion of the warrant and partially suppress the evidence obtained as a result of the defective portion of the warrant. *United States v. Billow,* 533 Fed.Appx. 757, 758 -760 (9th Cir. 2013) (explaining law on overbreadth and rejecting defendant's overbreadth challenge in a child pornography case).

Defendants appear to make several arguments on why the email search warrants were overbroad, all of which should be rejected. First, they appear to argue that the email service providers provided too much data to agents for their review. Defs. Br. at 9-10. Specifically, they argue "Attachment B includes all information related to the email and related content without any restriction." Defs. Br. at 9. Defendants' arguments are without merit.

The Ninth Circuit has consistently held, "[t]he number of files that could be scrutinized ... is not determinative. The search and seizure of large quantities of material is justified if the material is within the scope of the probable cause underlying the warrant." *United States v.*

*Hayes,* 794 F.2d 1348, 1355 (9th Cir. 1986). In the present case, the material was within the scope of the probable cause underlying the warrant. The email search warrants were justified in permitting the agents to review the data, in the various forms of information, within the email accounts.

Moreover, an agent's review of data and documents during the search which are ultimately unrelated to the evidence does not demand suppression of evidence. In any search it is inevitable that "some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those [items] authorized to be seized." *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). Similarly, the Ninth Circuit has concluded that "[t]he fear that agents searching a computer may come across such personal information cannot alone serve as the basis" for excluding evidence. *United States v. Adjani*, 452 F. 3d 1140, 1152 n.9 (9th Cir. 2006). To find otherwise would provide some form of heightened Fourth Amendment protection to computers, something the Ninth Circuit has rejected. *United States v. Giberson*, 527 F.3d 882, 888 (9th Cir. 2008) (potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's

reasonableness requirement); *accord United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008). The same analysis applies to email accounts.

As described in the affidavits, individuals involved with the advertisement, distribution, receipt, and accessing with intent to view child pornography often use email accounts to store, distribute and receive child pornography. Ex. A, pg. 13, last line. Such individuals rarely destroy contact lists of individuals they share child pornography with, along with the communications and images traded. Ex. A, pgs. 9-10 para. (c) & (d). Because the relevant information comes in a variety of forms (contact lists, substantive emails, and attached images, to name a few) it was wholly proper for the search warrant to permit agents to review numerous forms of information.

Similar to the present case, courts have upheld similar search warrants where the email service providers allowed agents to review numerous types of information and data within an email account, including countless emails. *See, e.g., Matter of Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp.3d 157, 159 -168 (D.D.C.2014) (reversing magistrate judge's decision denying an email search warrant

and finding agents were permitted to review all emails in an account to determine what should be seized). The mere fact that agents were permitted to search through a large amount of information does not make the warrant overbroad.[3] The Ninth Circuit has often recognized a legitimate law enforcement need to scoop up large quantities of data and sift through it carefully for concealed or disguised pieces of evidence. *See, e.g., United States v. Hill,* 459 F.3d 966 (9th Cir. 2006). Accordingly, the email cannot be deemed overbroad simply because there was a lot of material to review. The affidavit lays out sufficient probable cause to justify review of the various forms of data.

Defendants also complain that there were no date restrictions for the data to be searched within the email accounts. Again, defendants' arguments must fail. A review of the affidavit shows that individuals involved with the advertisement, distribution, receipt, and access with

---

[3] Agents are not required to search in the least restrictive manner. *See Vernonia Sch. Dist. 475J v. Acton*, 515 U.S. 646, 663 (1995) ("We have repeatedly refused to declare that only the 'least restrictive' search practicable can be reasonable under the Fourth Amendment."); *Quon v. Arch Wireless Operating Co., Inc*., 554 F.3d 769, 777-79 (9th Circ. 2009) (the use of the least restrictive means is not required, and Fourth Amendment does not require officers to use the best technique available as long as their method is reasonable under the circumstances). Reasonableness of the search is the ultimate standard under the Fourth Amendment. *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 539 (1967).

intent to view child pornography tend to retain their images of child pornography for many years. The images are rarely destroyed. Such images are often kept and distributed in their email accounts. Additionally, child pornographers often communicate with other individuals with an interest in child pornography over email and the communications and contacts are rarely destroyed. *See* Ex. A, pg. 9-10, para. (c ) and (d); pg. 13 (last sentence).

With those facts, there is probable cause to look at the entire account without a time restriction. In fact, it would be unreasonable to impose such a time restriction in an email account. For example, when agents execute a search warrant on a residence for child pornography in a peer –to-peer investigation, they are not restricted to images of child pornography uploaded on the P2P network during a certain week. Instead, they are permitted to look for any and all evidence of the child pornography, even if images were shared or possessed ten years prior.

In addition, the Supreme Court has held that the particularity requirement is relaxed when a complex scheme, such as this one, is under investigation. *Andresen v. Maryland*, 427 U.S. 463, 481 n.10 (1976). The breadth of the search warrant is also determined by the scope of the criminal activity. *United States v. Hernandez-Escarsega*,

886 F.2d 1560, 1568-69 (9th Cir. 1989) (warrant lawfully permitted seizure of virtually all the defendant's records because the affidavit established defendant used his legitimate business as a front for his illegal activities). The scope of the illegal activities and the length of the on-going child pornography conspiracy justified a less specific description of the items to be seized.

Defendants also seem to argue that the search warrant was overbroad because it permitted agents to obtain identity evidence. Defs. Br. at 10. The Ninth Circuit has repeatedly upheld warrants authorizing the seizure of items which establish the identity of persons in control of premises. "It is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects might contain the items described in the warrant." *United States v. Gomez–Soto,* 723 F.2d 649, 654 (9th Cir. 1994).

The Ninth Circuit has long upheld warrants "authorizing the seizure of items which establish the identity of persons in control of the premises." *United States v. Whitten,* 706 F.2d 1000 (9th Cir. 1983); (*citing United States v. Marques,* 600 F.2d 742, 751 at n.5 (9th Cir. 1979), *cert. denied,* 444 U.S. 1019 (1980)). Identity evidence connected

to the owner of an email account is no different. Identity evidence is part and parcel to any crime – if agents do not know the identity of the person engaged in criminal activity, there would be no individuals charged as criminal defendants in our criminal justice system. Because members of DMoon used screen-names while online, identity evidence was relevant to the investigation. Obtaining identity evidence was specifically outlined in Part II of Attachment B. It was wholly reasonable under the Fourth Amendment to obtain such information.

### B. Even if the Email Search Warrants Were Overbroad, the *Leon* Good Faith Exception Applies.

Assuming the email search warrants were overbroad (which they were not), agents reasonably relied on the search warrant papers. When analyzing overbreadth challenges, including in the email search warrant context, no Fourth Amendment violation occurs if the *Leon* "good faith" exception applies. *United States v. SDI Future Health, Inc.*, 568 F.3d 684 at 706.

"[I]n *United States v. Leon,* the Supreme Court set out an exception to the exclusionary rule for a search conducted in good faith reliance upon an objectively reasonable search warrant." *United States v. Crews,* 502 F.3d 1130, 1135–36 (9th Cir. 2007) (citing *United States v. Leon,* 468 U.S. 897, 925 (1984)). "Working from the premise that the

exclusionary rule is a judicially created, as opposed to constitutionally required remedy for Fourth Amendment violations, the Court reasoned that where police conduct is pursued in complete good faith, the rule's deterrent function loses much of its force." *United States v. Luong,* 470 F.3d 898, 902 (9th Cir. 2006). When it invokes the exception, the government bears the burden of proving that officers relied on the search warrant "in an objectively reasonable manner." *Crews,* 502 F.3d at 1136; *Luong,* 470 F.3d at 902 ("[T]he good faith test is an objective one."); *see also United States v. Michaelian,* 803 F.2d 1042, 1048 (9th Cir. 1986).

In the present case, agents provided the email search warrant papers to the Honorable Jeremiah C. Lynch for his review in the District of Montana. After reviewing the search warrant papers, Magistrate Lynch signed the warrants. When looking at search warrant papers themselves, which includes the detailed affidavits, and the fact that Magistrate Lynch reviewed and signed the warrants, agents relied on the search warrant in an objectively reasonable manner. Accordingly no items should be suppressed. *See, e.g., United States. v. Ingram,* 490 Fed.Appx. 363, 364-367 (2nd Cir. 2012)

(rejecting attacks of overbreadth in an email search warrant based on good faith exception).

### C. The Residential Search Warrants Contained Probable Cause to Search the Residences Without Reference to the Information From the Email Search Warrants; Thus, All Evidence and Statements Obtained From the Residential Search Warrants Are Admissible.

Defendants' attempts to suppress all evidence connected to the residential search warrants as a result of the email search warrants are far-fetched and unsupported by the case law. Defendants argue that identity evidence pertaining to Merchberger, Brown, Gustafson, and Edoria were improperly included in the residential search warrant and when such identity evidence is severed from the affidavits, no probable cause to search the residences existed. Defs. Br. at 10. A fair reading of each residential search warrant affidavit establishes that agents knew where the criminal activity was occurring based on the administrative subpoena returns and open source public records checks alone. *See* Ex. E (Merchberger) pg. 17, para. 31; Ex. F (Brown) pg. 40-41; Ex. G (Gustafson) pg. 31, para. (g) & (h); Ex. H (Edoria) pg. 22-23, para. 44-53.

Agents had probable cause to search the residences based solely on the location information from the subpoena returns and public record checks. Agents did not need to know who within the house was

engaging in the criminal activity in order to obtain a residential search warrant. While agents included some additional identity information in the residential search warrants suggesting who they believed within the house was engaged in criminal activity, that information was not key to the warrant. If such information is extracted, agents still had probable cause to search the residences.

Assuming, by some far off chance, probable cause did not exist for the residential search warrants, then the *Leon* good faith exception applies yet again. The agents presented detailed affidavits to their respective magistrate judges. The magistrate judges reviewed the materials and signed the warrants. It was objectively reasonable for the agents to rely on the residential search warrants.

## III. CONCLUSION

For all the reasons stated above, defendants motion to suppress should be denied.

DATED this 11th day of December, 2014.

**MICHAEL W. COTTER**
**United States Attorney**

*/s/ Maureen C. Cain*
Dept. of Justice Trial Attorney
**Cyndee L. Peterson**
Assistant United States Attorney

## CERTIFICATE OF COMPLIANCE

Pursuant to D. Mont. L.R. 7.1(d)(2) and CR 47.2, the attached GOVERNMENT'S RESPONSE TO MOTION TO SUPPPRESS is proportionately spaced, has a typeface of 14 points or more, and the body contains 3,243 words.

/s/ Cyndee L. Peterson
Assistant United States Attorney
Attorney for Plaintiff